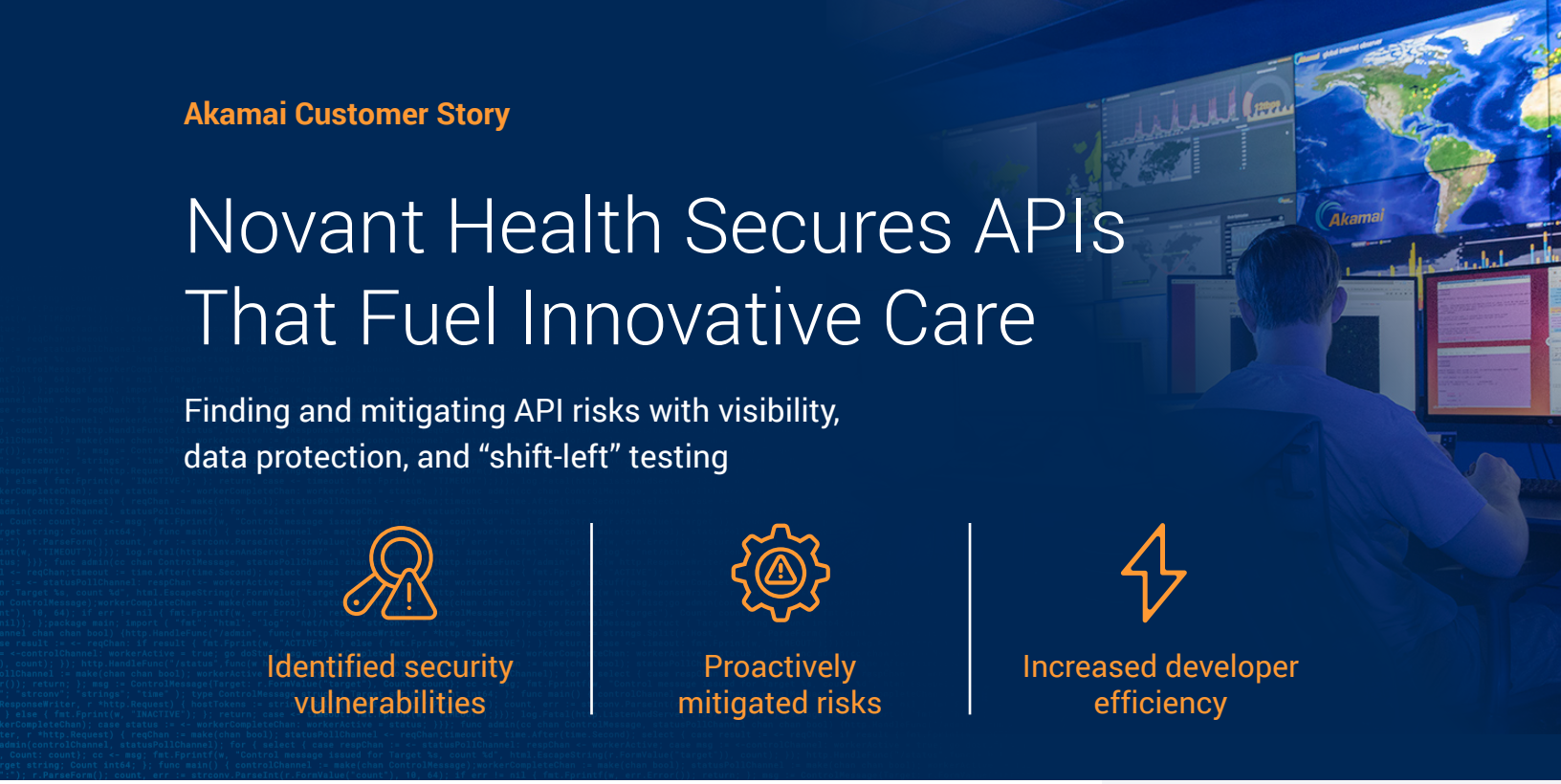
Akamai Customer Story

Novant Health Secures APIs That Fuel Innovative Care

Finding and mitigating API risks with visibility, data protection, and “shift-left” testing



Identified security vulnerabilities

Proactively mitigated risks

Increased developer efficiency

How many lives can a healthcare system improve through comprehensive, community-focused care? For Novant Health, the answer is staggering, including:

- 6.8 million physician clinic visits
- 155,964 inpatients cared for
- 602,590 emergency department visits
- 22,082 births

Numbers like these also provide a clear sense of who and what a healthcare institution needs to protect from threat actors that target sensitive data through API breaches.

Knowing what’s at stake

Novant Health is a not-for-profit integrated system of 16 medical centers and more than 1,900 physicians, spanning over 900 locations. With more than 36,000 team members and physician partners, the Winston-Salem–based organization provides care in North Carolina and South Carolina.

Through a range of digital initiatives, Novant makes patient care more effective, personalized, and efficient. APIs live at the core of this innovation, enabling a seamless exchange of patient data among applications, devices, and systems. In fact, APIs are so essential that Novant built a center of excellence (COE) that comprises the people, knowledge, and resources to ensure best-in-class API product development.

NOVANT HEALTH

Location

Winston-Salem, North Carolina
novanthealth.org

Industry

Healthcare and Life Sciences

Solution

API Security

Akamai

The team rightfully viewed API security as top priority from the outset, having researched how API-focused attacks impact healthcare providers. The industry statistics they uncovered along the way are also staggering, but not in a positive sense. For example, the average cost of a healthcare data breach is US$9.7 million. And 79% of healthcare organizations have experienced an API security incident in the past 12 months.

Pinpointing the problem

As a first order of business, the API COE determined that they needed to uplevel API security across Novant's entire organization. The sole solution they had in place was a web application firewall (WAF). These tools offer protection from already-known attacks, but today's healthcare organizations require a more comprehensive approach to securing APIs, including:

- Visibility into how many APIs exist within an organization's IT environment
- Insights on each API's risk attributes, such as types of data handled
- In-depth analyses of an organization's API-specific security posture, including uncovering misconfigurations that attackers exploit
- Protection from attacks that exploit flaws in API business logic

In addition, the Novant COE team identified key gaps in the organization's efforts to "shift left" or embed security into the early stages of development. They had tools in place for testing Docker containers, but needed a solution for the development of APIs. With sensitive data such as patient records on the line, the Novant COE team agreed they needed to find a vendor whose people and products were 100% focused on securing APIs.

Uncovering "ah-ha moments"

The Novant COE began meeting with Noname Security (now an Akamai company) after learning about its comprehensive approach to securing APIs. Together, they conducted an in-depth posture management analysis of every API in Novant's IT environment. Using the Noname API security platform (now part of Akamai API Security), the team identified an Azure vulnerability that held major security implications.

> "Akamai closed a considerable gap for us at Novant Health, allowing for clearer visibility into one of the most common assets targeted by malicious actors. The findings to date of actionable security vulnerabilities in our API ecosystem have already proven their value. At Novant Health, the protection of our data assets is our first priority. Akamai aligns with those values and has established itself as a foundational capability within our overall data security stack.
>
> – Justin P. Byrd
> Vice President, Data Platform and Integration, Novant Health

Akamai

The platform's API posture management solution revealed that some requests to APIs in Novant's cloud environment were coming in *around* their WAF tool, instead of through it. Threat attackers were bypassing the WAF through an "open door" the WAF couldn't secure and were repeatedly attacking Novant's APIs, leaving the company exposed and unaware.

The insights provided by Akamai were both shocking and immediately very helpful. Novant Health's ability to securely develop and maintain APIs hinges on having a fully protected cloud workspace. Novant's Vice President Justin P. Byrd and his team were impressed at how willing the Akamai team was to roll up their sleeves and apply their API posture management solution toward finding and mitigating the uncovered security gaps.

Building on their initial discoveries, the COE team can now use the Akamai API posture management solution's automated capabilities that continuously check APIs for misconfigurations and hidden risks, so the organization can take steps to proactively mitigate them. This includes the ability to identify which APIs and internal users are able to access sensitive data.

For an organization like Novant, which is a steward of health data that spans millions of patient interactions, knowing which APIs engage with sensitive information is critical – for building and sustaining trust with patients, providers, and regulators.

Realizing both security and business value

For the Novant COE — which comprises engineering leaders with hands-on experience — another priority was embedding security into the organization's API testing. Development speed is essential for every API, and that is especially true for an organization like Novant, whose APIs play a crucial role in patient care. However, the pressure to develop quickly also makes it easier for a vulnerability or design flaw to go undetected as developers race to production.

The COE sought reliable API testing capabilities to evaluate the security measures implemented into every API. This involves conducting comprehensive tests to identify weaknesses in variables such as authentication mechanisms, authorization controls, data integrity, and encryption protocols.

Of course, with any implementation of a new security tool, success relies not only on functionality, but also on engagement with key stakeholders. Developers understand the importance of security, but given their need for speed, they're typically wary of any slowdowns that an unfamiliar tool could bring.

Such was the case at Novant Health — at first.

As the Novant team further engaged with Akamai, it determined a range of capabilities that could help developers do their jobs securely, and in ways that create efficiencies. For example, Akamai API Security's Active Testing could proactively uncover mistakes that would have become significant, time-consuming problems later in the process.

In addition, the solution also enabled the COE to give developers quick notes to drive efficiency — a pleasant surprise for COE team members who didn't realize the solution also did nonsecurity QA checks. For example, they could now determine whether an API's specs matched what the built APIs were actually providing. It wasn't long before the developers — who were lukewarm at first — joined the COE team in realizing the benefits to security and efficiency and became excited about working with Akamai API Security.

"From day one, Akamai has been a trusted advisor on how to discover, protect, and test our APIs spanning all stages, from coding to production. This enables our center of excellence to show the entire organization how to achieve security and efficiency, all at once," explained Byrd. "This partnership is about more than products; the people on the Noname [now an Akamai company] team understand our world and the business drivers behind API development."

Novant's leadership also agreed, citing Akamai API Security's ability to "catch things before they become a problem," and helped cement API security into the organization's shift-left efforts.

Building on API security gains

Today, Novant uses Akamai API Security to provide “automatic protection” for their APIs and every digital initiative they power. Building on Novant’s gains in discovering, inventorying, assessing, and testing APIs, the COE team is now applying the platform’s comprehensive protection to new APIs that Novant develops. The team believes that as Novant developers build APIs based on aligned best practices, each API will be automatically protected.

Looking ahead, the COE team envisions expanding the use of the Akamai API Security to other teams within the company. Aiming for a cross-enterprise collaborative model for API protection, the COE envisions a partnership among themselves, the Novant Health security team, and the organization’s foundation structure team in using Akamai API Security.

NOVANT HEALTH

Novant Health is a not-for-profit integrated system of 19 medical centers and more than 2,000 physicians in over 900 locations, as well as numerous outpatient surgery centers, medical plazas, rehabilitation programs, diagnostic imaging centers, and community health outreach programs. Novant Health’s nearly 40,000 team members and physician partners care for patients and communities in North Carolina and South Carolina.

| Published 01/25

Akamai